Shielded Transfers

CONCORDIUM

The Concordium Platform supports shielded transfers, which hide the transferred amount from anybody except the sender and the receiver. To allow for shielded transfers, accounts have a shielded balance in addition to their public balance. Only the account holder can see the value of the shielded balance. A shielded transfer has the same functionality as a plain transfer except that it operates on the shielded balances and the transferred amount is hidden and only known to the sender and receiver. To ensure that the sender has a sufficient shielded balance, the transaction contains a zero-knowledge proof that allows everyone to verify that the amount in the transfer does not exceed the sender's shielded balance, without revealing any of these values.

The anonymity revokers are able to reveal shielded amounts if instructed by the authorities in a process similar to that used for anonymity revocation.

Shielding Parts of the Public Balance

Users can shield parts of the public balance on one of their accounts by encrypting the corresponding amount. The encrypted value is then added to the set of encrypted balances of that user and the corresponding amount is deducted from their public balance. Since the deducted amount is public, the encrypted amount is also public at this point. The encryption can therefore be done with fixed randomness so that it is publicly verifiable that the correct amount was encrypted.

Unshielding Parts of the Private Balance

Users can make parts of their shielded balance public again. If their shielded balance consists of multiple ciphertexts S_i, they are first aggregated into a single ciphertext S encrypting the sum $s = s_1 + s_2 + \ldots + s_n$ of the individual values s_i using a homomorphic property of the encryption scheme. The user then creates a new ciphertext S' encrypting the value $s' = s - a$, where $a \geq 0$ is the value the user wants to make public. Finally, the user generates a non-interactive zero-knowledge proof showing that S' is indeed a valid encryption of a value s' such that $s' = s - a$ and $s' \geq 0$. The bakers can then verify the validity of the zero-knowledge proof. The new shielded balance ciphertext of the user becomes S' and the value a is added to the user's public balance.

Shielded Transfers Between Different Accounts

Shielded transfers from an account X to an account Y work similarly to unshielding amounts: The account holder of account X aggregates all ciphertexts of X's shielded balance into a single ciphertext S and encrypts the value $s' = s - a$ in a ciphertext S', where a is the amount to be transferred to account Y. Since the amount a here also should remain hidden, it is additionally encrypted in a ciphertext A. The zero-knowledge proof then in addition to showing $s' = s - a$ and $s' \geq 0$ also needs to show that A is a valid encryption of the secret value $a \geq 0$. After the transfer, the shielded balance of account X becomes S', and the ciphertext A is added to the shielded balance of account Y.

Opening Shielded Amounts by Anonymity Revokers

Given a court order from a qualified authority, the anonymity revokers are able to open the shielded balances of the affected accounts. This also allows them to unshield the amounts of all incoming and outgoing transactions from that account. This is achieved by storing the decryption key of an account encrypted under the public keys of the anonymity revokers on chain when opening an account. The correctness of this encryption is again proven in zero-knowledge by the user opening the account and verified by the bakers.

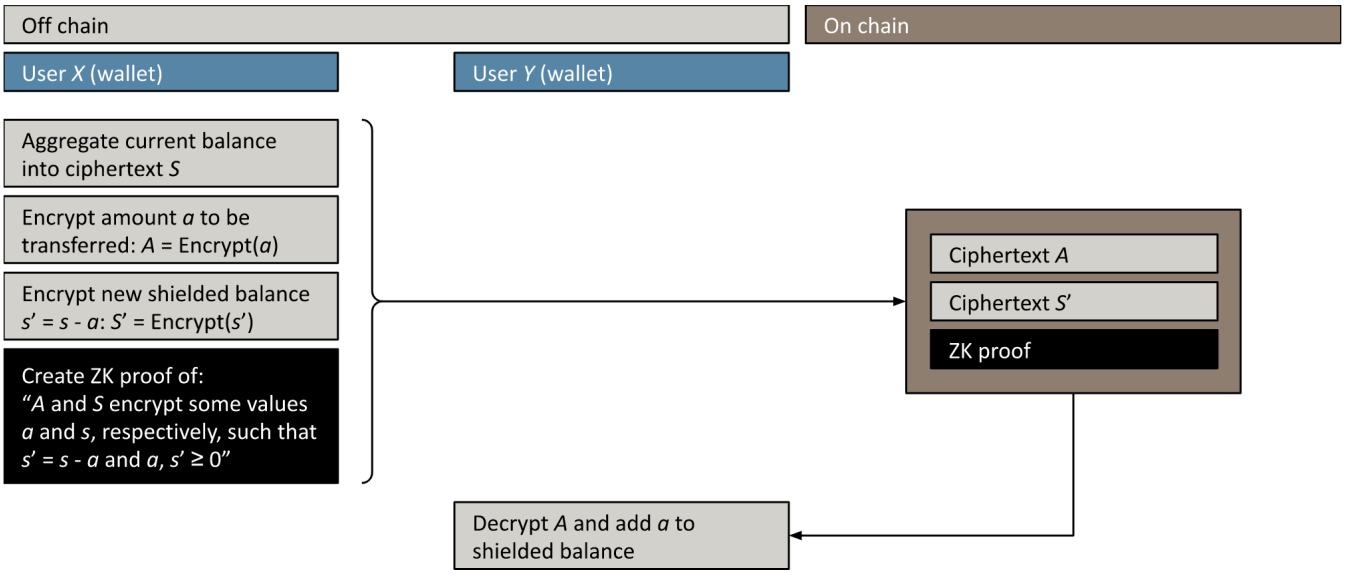

Figure: Encrypted transfer (simplified) of amount *a* from user *X* to user *Y*, where *s* and *s'* are the shielded balances of *X* before and after the transaction, respectively.